IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF PUERTO RICO

COMMONWEALTH OF PUERTO RICO, Plaintiff, vs. EQUIFAX, INC, Defendant.	Case No. _____ COMPLAINT AND DEMAND FOR JURY TRIAL

I. INTRODUCTION

1. The Commonwealth of Puerto Rico ("Puerto Rico") brings this action in its sovereign capacity against Equifax, Inc. ("Equifax") on behalf of itself and as *parens patriae* on behalf of the population of Puerto Rico.

2. Equifax is one of three primary national credit-reporting bureaus in the United States. Equifax collects and maintains data regarding more than 820 million consumers worldwide, including at least one million residents of Puerto Rico. The personal data that Equifax holds touches upon virtually every aspect of a consumer's profile in the marketplace.

3. Equifax is a gatekeeper for consumers' access to socioeconomic opportunity and advancement. Every day, businesses across the world rely on Equifax's credit profiles to make decisions as to the credit worthiness of consumers. This information impacts many of the most important decisions in the lives of consumers—for instance, whether consumers can buy a house, obtain loans, lease vehicles, or even get a job.

4. Consumers do not have any reasonable manner of preventing Equifax from collecting, processing, using or disclosing their private information. Equifax largely controls how,

when, and to whom the consumer data it stockpiles is disclosed. Likewise, consumers have no choice but to rely on Equifax to protect their most sensitive and personal data.

5. Equifax must, above all else, protect highly sensitive personal and financial information that it collects from consumers. When a consumer's information is collected by Equifax, Equifax must be at the absolute forefront of data security to ensure that thieves and hackers cannot access the data it has collected.

6. Equifax cannot, as it did here, fail to patch critical software effectively and promptly, especially when such solutions are available, and even more so when exploits based on the vulnerability in that software have been widely reported. When a data breach involving up to 143 million records of innocent consumers occurs, Equifax must immediately and accurately notify all those affected to prevent consumers from becoming victims of identity theft. And it must take immediate steps to mitigate the damages it has caused, rather than half-steps that could lead to self-enrichment. This Complaint stems from Equifax's abject failure to follow these simple steps.

7. From at least March 7, 2017 through July 30, 2017, a period of almost five months, Equifax left at least 143 million consumers' sensitive and private information exposed and vulnerable to thieves and hackers by relying on certain open-source code (called "Apache Struts") that Equifax knew or should have known was insecure and subject to exploitation. Although patches, workarounds, and other fixes for the vulnerability were available and known to Equifax as of March 7, 2017, Equifax failed to utilize these public and available remedies or employ proper security controls, such as encryption or multiple layers of security, that were sufficient to protect consumers' personal data.

8. As a result, intruders were able to access Equifax's computer system from at least May 13, 2017 through July 30, 2017, and potentially stole the sensitive and personal

information of 143 million consumers (the "Data Breach"). The Data Breach, which Equifax first disclosed to the public months later on September 7, 2017, exposed some of the most sensitive and personal data of Puerto Rico residents, including full names, Social Security numbers, dates of birth, addresses, and, for some, credit card numbers, driver's license numbers, and/or other unknown, confidential information collected or generated incident to Equifax's business.

9. Equifax could have—and should have—prevented the Data Breach had it implemented and maintained reasonable safeguards, consistent with representations made to the public in its advertisements. Equifax did not do so.

10. By failing to protect confidential consumer information, Equifax exposed ***over half of the adult population of Puerto Rico*** to the risk of identity theft, tax return scams, financial fraud, health identity fraud, and other harm. Affected consumers have spent, and will continue to spend, money, time, and other resources attempting to protect against an increased risk of identity theft or fraud, including by placing security freezes over their credit files and monitoring their credit reports, financial accounts, health records, government benefit accounts, and any other account tied to or accessible with a social security number. The increased risk of identity theft and fraud as a result of the Data Breach also has caused Puerto Rico consumers substantial fear and anxiety and likely will do so for many years to come.

11. Given the nature of Equifax's business, the sensitivity and volume of the data in which it traffics, and the serious consequences to consumers when that data is exposed, its failure to secure this information constitutes a shocking betrayal of public trust and an egregious violation of Puerto Rico consumer protection and data privacy laws. As Equifax's

own Chairman and Chief Executive Officer admitted, the Data Breach "strikes at the heart of who we are and what we do."

12. By this action Puerto Rico seeks to ensure that Equifax is held accountable, and not allowed to prioritize profits over the safety and privacy of consumers' sensitive and personal data. Puerto Rico seeks, in its capacity as *parens patriae*, to recover individual damages suffered by all natural persons in Puerto Rico as a result of Equifax's misconduct. Puerto Rico also seeks disgorgement of profits, restitution, costs, and attorney's fees. Puerto Rico also seeks appropriate, and available equitable and injunctive relief to address, remedy, and prevent harm to Puerto Rico residents resulting from Equifax's actions and inactions.

II. THE PARTIES

13. The Plaintiff is the Commonwealth of Puerto Rico, who brings this action on behalf of itself and as *parens patriae* on behalf of Puerto Rico residents, under the laws of Puerto Rico, to ensure compliance with Puerto Rican laws and to enjoin violations of Puerto Rican laws.

14. Defendant Equifax, Inc. is a publicly-traded Georgia corporation (NYSE: EFX) with its principal place of business at 1550 Peachtree Street N.E. in Atlanta, Georgia.

III. JURIDICTION AND VENUE

15. This Court has diversity jurisdiction over this action under 28 U.S.C. § 1332(a)(3). Plaintiff and Defendant are citizens of different states. The amount in controversy exceeds $75,000, exclusive of interest and costs.

16. This Court has personal jurisdiction over Equifax because Equifax regularly conducts business in Puerto Rico, has minimum contacts with Puerto Rico, and maintains a place of business in this District.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Puerto Rico resides in this District, a substantial part of the events or omission giving rise to these claims occurred in this District, and Equifax has caused harm to Puerto Rico residents who reside in this District.

IV. FACTS

A. Equifax

18. Equifax was founded in 1899 and is the oldest of the "big three" credit reporting agencies based in the United States. Equifax's stock is listed on the New York Stock Exchange under the ticker symbol "EFX." In its 2016 Annual Report, Equifax claimed operating revenue of $3.145 billion and operating income of $818 million.

19. Equifax's business centers on the collection, processing, and sale of information about people and businesses. According to its website, Equifax is a global information solutions company that organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide.

20. According to statements filed with the United States Securities Exchange Commission ("SEC"), Equifax accumulates a staggering array of the private personal information of millions of Puerto Rican residents for the purpose of enabling businesses "to make credit and service decisions, manage their portfolio risk, automate or outsource certain human resources, employment tax and payroll-related business processes, and develop marketing strategies concerning consumers and commercial enterprises." Equifax acknowledges that this information includes "credit, income, employment, asset, liquidity, net worth and spending activity, and business data, including credit and business demographics that we obtain from a variety of sources,

such as credit granting institutions, public record information, income and tax information primarily from large to mid-sized companies in the U.S., and survey-based marketing information."

21. Additionally, as part of its business, Equifax creates, maintains, and sells credit reports and credit scores regarding individual Puerto Rican residents. Credit reports can contain, among other things, an individual's full Social Security number, current and prior addresses, age, employment history, detailed balance and repayment information for financial accounts, bankruptcies, judgments, liens, and other sensitive information. The credit score is a proprietary number, derived from a credit report and other information that is intended to indicate relative to other persons whether a person would be likely to repay debts.

22. Third parties use credit reports and credit scores to make highly consequential decisions affecting Puerto Rican consumers. For instance, credit scores and/or credit reports are used to determine whether an individual qualifies for a mortgage, car loan, student loan, credit card, or other form of consumer credit; whether a consumer qualifies for a certain bank account, insurance, cellular phone service, or cable or internet service; the individual's interest rate for the credit they are offered; the amount of insurance premiums; whether an individual can rent an apartment; and even whether an individual is offered a job.

23. Equifax is acutely aware that the consumer and business information it stores is highly sensitive and highly valuable to identity thieves and other criminals. On its website, Equifax states:

> **Privacy**
>
> For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses.

> We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

There is little question that the above policy demonstrates Equifax was well aware of the need for it to protect consumers' highly valuable personal and financial information.

B. The Data Breach

24. At all relevant times, Equifax maintained a publicly-available website at www.equifax.com. Within that website are various publicly-available web pages directed to consumers, including Puerto Rican residents. Among those web pages is one through which Equifax invites consumers to submit information to initiate and support a formal dispute of information in their credit reports (the "Dispute Portal").

25. Equifax maintained consumer names, addresses, full Social Security numbers, dates of birth, and for some consumers, driver's license numbers, credit card numbers, and other confidential information of at least one million Puerto Rican residents, in computer tables, databases, or files that were accessible (directly or indirectly) through the Dispute Portal (the "Exposed Information"). The Exposed Information was not limited to the sensitive and personal information of those consumers who had used the Dispute Portal, but encompassed a larger group of consumers on whom Equifax held information.

26. Starting on or about May 13, 2017 through July 30, 2017, unauthorized third parties infiltrated Equifax's computer system via the Dispute Portal. Once in, the parties accessed and stole Exposed Information from Equifax's network. According to a statement Equifax published online at https://www.equifaxsecurity20l7.com on or about September 13,

2017, the Data Breach resulted when "criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638."

27. Apache Struts is a piece of computer code used for creating web applications. That is, a computer program that runs in a web browser.

28. At all relevant times, Equifax used Apache Struts, in whole or in part, to create, support, and/or operate its Dispute Portal.

29. Apache Struts is a piece of software that is free and available for anyone to download, install, or otherwise integrate into their computer system. Apache Struts, like many other pieces of open-source code, comes with no warranties of any kind including warranties about its security. Accordingly, it is incumbent on companies that use Apache Struts—like Equifax—to assess whether the open-source code is appropriate and sufficiently secure for the company's purposes and that it is kept up-to-date and secure against known vulnerabilities.

30. There are, and at all relevant times have been, multiple well-known resources available to support companies relying on open-source code, including Apache Struts. These resources publicly announce to users when security vulnerabilities in the open-source code are discovered and verified, including in Apache Struts, compare the associated risks of such vulnerabilities, and propose fixes.

31. For example, the Apache Software Foundation ("Apache"), a non-profit corporation, releases updated versions of Apache Struts to "patch" it against verified security vulnerabilities. Apache also releases Security Bulletins on its website regarding security flaws in Apache Struts, noting the nature of the vulnerability and ways to resolve it. Since 2007, Apache has posted at least 53 such security bulletins for Apache Struts.

32. Similarly, the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") maintains a free and publicly available National Vulnerability Database ("NVD") at http://nvd.nist.gov. Using the NVD, NIST identifies security vulnerabilities, including in open-source code, the risks they pose, and ways to fix them, including as to security vulnerabilities in Apache Struts.

33. Likewise, the MITRE Corporation, a "not-for-profit organization that operates research and development centers sponsored by the [United States] federal government," also identifies code security vulnerabilities, including vulnerabilities in Apache Struts, using a Common Vulnerabilities and Exposures ("CVE") Identifier. According to MITRE, the CVE Identifier is the industry standard for identifying publicly known cyber security vulnerabilities. MITRE maintains a database of CVE identifiers and the vulnerabilities to which they correspond, which is publicly accessible without cost online at https://cve.mitre.org (the "Vulnerability Database").

34. On March 7, 2017, Apache published notice of a security vulnerability in certain versions of Apache Struts in its online security bulletins S2-045 and S2-046 (the "Apache Security Bulletins"). The vulnerability was assigned the CVE identifier CVE- 2017-5638 (the "March Security Vulnerability").

35. Directed to "All Struts2 developers and users," the Apache Security Bulletins warned that the software was vulnerable to "Remote Code Execution," or "RCE." RCE refers to a method of hacking a public website whereby an online attacker can send computer code to the website that allows the attacker to infiltrate (that is, gain access to), and run commands on the website's server (the computer that stores the information that supports the website).

36. The Apache Security Bulletins assigned the March Security Vulnerability a "maximum security rating" of "***critical***." Apache recommended that users update the affected

versions of Apache Struts to fix the vulnerability, or to implement other specific workarounds to avoid the vulnerability.

37. NIST also publicized the March Security Vulnerability in its NVD on or about March 10, 2017. ("NIST Notice"). NIST noted that the severity of the vulnerability was an overall score of 10.0 on two different versions of a scale called the Common Vulnerability Scoring System ("CVSS"). A score of 10.0 is the highest possible severity score on either scale. The NIST Notice also stated that an attack based on the vulnerability "[a]llows unauthorized disclosure of information," would be low in complexity to accomplish, and would not require the attacker to provide authentication (for example, a user name and password) to exploit the vulnerability. The NIST Notice also documented over twenty other online resources for advisories, solutions, and tools related to the March Security Vulnerability and how to patch or fix it.

38. Following the NIST Notice, the United States Computer Emergency Readiness Team ("US CERT") issued a security Bulletin (Bulletin (SB17-079)) on March 20, 2017, calling out the March Security Vulnerability as a "High" severity vulnerability ("US CERT Alert").

39. Likewise, MITRE included the March Security Vulnerability in the Vulnerability Database and documented various external website references to the March Security Vulnerability.

40. In the days following the public disclosure of the March Security Vulnerability by Apache, media reports claimed that hackers were exploiting the March Security Vulnerability against numerous companies, including banks, government agencies, internet companies, and other websites.

41. As Equifax disclosed to the public on its website on or about September 13, 2017, the Data Breach occurred as a result of the exploitation of the March Security Vulnerability by hackers.

42. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that the March Security Vulnerability existed in Apache Struts.

43. Indeed, in a notice on the website https://www.equifaxsecurity20l7.com/, Equifax stated that "Equifax's Security organization was aware of this vulnerability" in Apache Struts in early March 2017.

44. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that the implementation of Apache Struts it employed on its websites, including without limitations, the Dispute Portal was susceptible to the March Security Vulnerability.

45. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that it was vulnerable to unauthorized access to sensitive and personal consumer information by exploitation of the March Security Vulnerability by hackers.

46. Until at least July 30, 2017, and during the Data Breach, Equifax continued to use an Apache Struts-based web application that was susceptible to the March Security Vulnerability for its Dispute Portal.

47. Until at least July 30, 2017, and during the Data Breach, Equifax failed to employ successfully recommended fixes or workarounds, otherwise patch or harden its systems, or put in place any compensating controls sufficient to avoid the March Security Vulnerability, safeguard the Exposed Information, or prevent the Data Breach.

48. In addition, until at least July 29, 2017, and during the Data Breach, Equifax did not detect and/or appropriately respond to evidence that unauthorized parties were infiltrating its computer systems and had access to the Exposed Information; and/or did not detect or appropriately respond to evidence that those parties were exfiltrating the Exposed Information out of Equifax's computer system.

49. As a result of Equifax's actions and inactions, the Data Breach occurred and hackers were able to access and stole the confidential, sensitive and personal information of residents of Puerto Rico.

50. In its Form 8-K filing with the SEC on May 4, 2018, Equifax admitted that the Social Security Numbers of ***more than 99% of individuals affected*** were compromised. The full extent of personal data exposed as a result of the Equifax Data Breach is reproduced below, as described in Equifax's Form 8-K:

Data Element Stolen	Standardized Columns Analyzed [1]	Approximate Number of Impacted U.S. Consumers
Name	First Name, Last Name, Middle Name, Suffix, Full Name	146.6 million
Date of Birth	D.O.B.	146.6 million
Social Security Number [2]	SSN	145.5 million
Address Information	Address, Address2, City, State, Zip	99 million
Gender	Gender	27.3 million
Phone Number	Phone, Phone2	20.3 million
Driver's License Number [3]	DL#	17.6 million
Email Address (w/o credentials)	Email Address	1.8 million
Payment Card Number and Expiration Date	CC Number, Exp Date	209,000
TaxID	TaxID	97,500
Driver's License State	DL License State	27,000

Equifax, Form 8-K (May 4, 2018) at 2, *available at* https://investor.equifax.com/financial-information/sec-filings (last visited June 28, 2018)

51. Equifax knows that it was not doing enough to protect the sensitive information it had in its possession. Equifax's Chairman and CEO Richard F. Smith admits: "Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will." But promises to do better in the future will not help the consumers whose identities have already been compromised.

C. Equifax's Security Program Fell Short

52. At all relevant times, Equifax promised the public that safeguarding consumers' sensitive, personal information is "a top priority." Common sense dictates that credit bureaus, which maintain custody of critical private personal information for millions of consumers are a prime target of hackers who are either engaged in identity theft or who seek to profit by selling private consumer information to identity thieves.

53. Equifax's knowledge of the risks of data breaches is highlighted by the fact that Equifax profits off of consumer fears of such breaches. Equifax markets identity theft protection services directly to people who believe their confidential information has been involved in a data breach, telling them: "If you've recently been notified that your information was involved in a data breach, you likely have a lot of questions. We're here to help answer those questions and help you understand the steps you may take to help better protect your identity in the future." The Equifax website counsels people whose information has been hacked that "it is wise to consider taking advantage of the credit monitoring product, if it is offered." And the very same page advertises Equifax's own "Equifax ID Patrol" and "Equifax Complete Family Plan" products to people, assuring them that "a surprise-free future starts here."

54. Equifax profited handsomely from consumer fears of identity theft and data breaches. As reported in Equifax's filings with the SEC, during the first six months of 2017 alone,

Equifax earned more than $205 million in operating revenue from its "Global Consumer Solutions" segment, which includes revenue generated from "credit information, credit monitoring and identity theft protection products sold directly and indirectly to consumers via the internet and in various hard-copy formats. . . ."

55. Despite its knowledge of the risks of a data breach, and despite its knowledge of the critical nature of the information that it collects, stores, and maintains, Equifax failed to take adequate and reasonably necessary steps to protect the information in its possession.

56. The profound impact of the Equifax Data Breach has been highlighted by the cybersecurity industry. In a post titled, "Why the Equifax breach is very possibly the worst leak of personal info ever," Ars Technica writer Dan Goodin noted that "[c]onsumers' most sensitive data is now in the open and will remain so for years to come." Goodin described the Equifax Data Breach as "very possibly [] the most severe of all for a simple reason: the breathtaking amount of highly sensitive data it handed over to criminals. By providing full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers, it provided most of the information banks, insurance companies, and other businesses use to confirm consumers are who they claim to be. The theft, by criminals who exploited a security flaw on the Equifax website, opens the troubling prospect that the data is now in the hands of hostile governments, criminal gangs, or both and will remain so indefinitely."

D. Equifax Failed To Notify The Public For Months That Their Personal Data Had Been Compromised

57. Puerto Rico residents clearly have already suffered significant and lasting harm as a result of the Data Breach, and such harm is likely to continue and worsen over time.

58. Armed with an individual's sensitive and personal information—including in particular a social security number, date of birth, and/or a drivers' license number—a criminal

can commit identity theft, financial fraud, and other identity-related crimes. According to the Federal Trade Commission ("FTC"):

> Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

59. Identity theft results in real financial losses, lost time, and aggravation to consumers. In its 2014 Victims Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of the total identity theft victims never had those losses reimbursed. The average out-of-pocket loss for those victims was $2,895. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings." With respect to consumers' emotional distress, the report also noted that more than one-third of identity theft victims were moderately or severely distressed due to the crime.

60. The Data Breach has substantially increased the risk that the affected Puerto Rico consumers will be a victim of identity theft or financial fraud at some unknown point in the future.

61. In order to protect themselves from this increased risk of identity theft and fraud, many consumers may place "security freezes" on their credit reports with one or more consumer reporting agency, including Equifax. The primary objective of a security freeze is to prevent third parties from accessing the frozen credit report when a new application for credit is placed without the consumer's consent.

62. As a result of Equifax's actions and inactions in connection with the Data Breach, and in an effort to protect themselves against identity theft or financial fraud, many Puerto Rico consumers have already spent and will continue to spend time and money in an effort to place security freezes on their credit reports with Equifax and other consumer reporting agencies.

63. Further, Equifax has complicated consumers' efforts to protect themselves from the harms caused by the Data Breach by failing to take various measures that it was uniquely positioned to take to mitigate the risk of harm caused by the Data Breach. Instead, Equifax has failed to clearly and promptly notify consumers whether they were affected by the Data Breach, has charged consumers to place security freezes (and presumably unfairly profited thereby), has failed to offer consumers free credit and fraud monitoring beyond one year, and has failed to ensure adequate call center staffing and availability of online services in the days following the September 7, 2017 announcement of the Data Breach. Equifax's actions and inactions in this regard have compounded the harms already suffered by consumers.

CAUSES OF ACTION

COUNT I

Negligence
(on behalf of the Puerto Rican Aggrieved Individuals)

64. Puerto Rico incorporates the allegations in the proceeding paragraphs as if fully set forth herein.

65. Equifax owed a duty to all natural persons in Puerto Rico whose personal, confidential information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017, excluding Defendants their affiliates, subsidiaries co-

conspirators, employees (including its officers and directors) ("the Puerto Rican Aggrieved Individuals").

66. Specifically, Equifax owed a duty to the Puerto Rican Aggrieved Individuals to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their personal and financial information in its possession from being compromised, lost stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's security system to ensure that their personal and financial information in Equifax's possession was adequately secured and protected. Equifax further owed a duty to the Puerto Rican Aggrieved Individuals to implement processes that would detect a breach of it security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

67. Equifax owed a duty to the Puerto Rican Aggrieved Individuals to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of the Puerto Rican Aggrieved Individuals.

68. Equifax owed a duty of care to the Puerto Rican Aggrieved Individuals because they were foreseeable and probable victims of any inadequate security practices. Equifax solicited, gathered, and stored the personal and financial data of the Puerto Rican Aggrieved Individuals to facilitate credit reports and monitoring. Equifax knew it inadequately safeguarded such information on its computer systems and that hackers routinely attempt to access this valuable data without authorization. Equifax had prior notice that its systems were inadequate by virtue of the earlier breaches that preceded this one, but continued to maintain those inadequate systems to the ultimate detriment of its customers like the Puerto Rican

Aggrieved Individuals. Equifax knew or should have known that a breach of its systems would cause damages to the Puerto Rican Aggrieved Individuals and Equifax had a duty to adequately protect such sensitive personal and financial information.

69. Equifax owed a duty to timely and accurately disclose to the Puerto Rican Aggrieved Individuals that their personal and financial information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate, and necessary so that, among other things, the Puerto Rican Aggrieved Individuals could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Equifax's misconduct.

70. Equifax knew, or should have known, the risks inherent in collecting and storing the personal and financial information of the Puerto Rican Aggrieved Individuals, and of the critical importance of providing adequate security of that information.

71. Equifax's own conduct also created a foreseeable risk of harm to the Puerto Rican Aggrieved Individuals. Equifax's misconduct included, but was not limited to, its failure to take steps and opportunities to prevent and stop the data breach as set forth herein.

72. Equifax breached the duties it owed to the Puerto Rican Aggrieved Individuals by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal and financial information of the Puerto Rican Aggrieved Individuals.

73. Equifax breached the duties it owed to the Puerto Rican Aggrieved Individuals by failing to properly implement technical systems or security practices that could have prevented the loss of data at issue.

74. Equifax breached its duties to timely and accurately disclose that the Puerto Rican Aggrieved Individuals' personal and financial information in Equifax's possession had been or was reasonably believed to have been stolen or compromised.

75. But for Equifax's wrongful and negligent breach of its duties owed to the Puerto Rican Aggrieved Individuals, their personal and financial information would not have been compromised.

76. The injury and harm suffered by the Puerto Rican Aggrieved Individuals, as set forth above was the reasonably foreseeable result of Equifax's failure to exercise reasonable care in safeguarding and protecting the Puerto Rican Aggrieved Individuals' personal and financial information within Equifax's possession. Equifax knew or should have known that its systems and technologies for processing, securing, safeguarding, and deleting the Puerto Rican Aggrieved Individuals' personal and financial information were inadequate and vulnerable to being breached by hackers.

77. The Puerto Rican Aggrieved Individuals suffered injuries and losses described herein as a direct and proximate result of Equifax's conduct resulting in the data breach, including Equifax's lack of adequate reasonable and industry-standard security measures. Had Equifax implemented such adequate and reasonable security measures, the Puerto Rican Aggrieved Individuals would not have suffered the injuries alleged, as the Equifax data breach would likely have not occurred.

78. A special relationship exists between the Puerto Rican Aggrieved Individuals and Equifax.

79. Equifax collects personal and financial data from the Puerto Rican Aggrieved Individuals to create credit scores and monitor credit activity, including during the period of the Equifax data breach. The Puerto Rican Aggrieved Individuals allowed this to happen with the understanding that Equifax had reasonable security measures in place to protect its customers' personal and financial information.

80. Equifax's conduct warrants moral blame, as Equifax continued to take possession of the Puerto Rican Aggrieved Individuals' personal and financial information in connection with its Services knowing, and without disclosing, that it had inadequate systems to reasonably protect such information and even after the data breach had occurred and was ongoing, and Equifax failed to provide timely and adequate notice to the Puerto Rican Aggrieved Individuals as required by law.

81. Holding Equifax accountable for its negligence will further the policies underlying negligence law and will require Equifax and encourage similar companies that obtain and retain sensitive consumer personal and financial information to adopt, maintain and properly implement reasonable, adequate and industry-standard security measures to protect such customer information.

82. As a direct and proximate result of Equifax's negligent conduct, Puerto Rican Aggrieved Individuals' have suffered injury and are entitled to damages in the amount to be proven at trial.

83. A sovereign entity such as Puerto Rico may proceed as *parens patriae* to recover damages on behalf of its population if it 1) articulates an interest apart from the

interests of particular private parties, (2) expresses a quasi-sovereign interest, and (3) alleges injury to a sufficiently substantial segment of its population. *Alfred L. Snapp & Son v. Puerto Rico*, 458 U.S. 592, 600 (1982).

84. Puerto Rico has its own interest in protecting the rights of its population, including consumers, from deceptive misrepresentations about the nature and quality of services and actions or inactions that may harm its population, directly harming the current population and indirectly chilling the desire of others to visit or reside in Puerto Rico. That interest is distinct from the interest of consumers themselves in avoiding harm as a result of such misrepresentations, actions or inactions. The foregoing is a sovereign interest.

85. A substantial segment of Puerto Rico's population was affected by Equifax's misconduct. At least 1,000,086 people, or ***more than half*** of Puerto Rico's adult population, were affected as a result of Equifax's misconduct.

86. Accordingly, Puerto Rico may proceed as *parens patriae* to recover damages on behalf of its population.

PRAYER FOR RELIEF

WHEREFORE, Puerto Rico requests that the Court grant the following relief:

1. Order Equifax to pay monetary damages suffered by the Puerto Rican Aggrieved Individuals as a result of Equifax's negligence, in an amount to be proven at trial;

2. Order that Equifax pay the costs of investigation and litigation of this matter, including reasonable attorneys' fees, to Puerto Rico in an amount to be determined at trial;

3. Disgorge profits Equifax obtained during or as a result of the Data Breach: and

4. Order such other just and proper legal and equitable relief.

REQUEST FOR JURY TRIAL

Puerto Rico hereby requests trial by jury as to all issues so triable.

Dated: June 28, 2018

Respectfully Submitted,

/s Denise Maldonado Rosa
Wanda Vázquez-Garced
Attorney General

Denise Maldonado Rosa
Assistant Attorney General
USDC-PR 301108
P.O. Box 9020192
San Juan, Puerto Rico 00902-0192
Tel: (787) 729-2002
dmaldonado@justicia.pr.gov

/s Peter B. Schneider
Peter B. Schneider
SCHNEIDER WALLACE COTTRELL KONECKY WOTKYNS LLP
3700 Buffalo Speedway, Suite 300
Houston, Texas 77098
Telephone: (713) 338-2560
Facsimile: (415) 421-7105
pschneider@schneiderwallace.com

/s Todd M. Schneider
Todd M. Schneider
Kyle G. Bates
SCHNEIDER WALLACE COTTRELL KONECKY WOTKYNS LLP
2000 Powell St., Suite 1400
Emeryville, California 94608
Telephone: (415) 421-7100
Facsimile: (415) 421-7105
tschneider@schneiderwallace.com
kbates@schneiderwallace.com

/s Garrett W. Wotkyns
Garrett W. Wotkyns

SCHNEIDER WALLACE COTTRELL KONECKY WOTKYNS LLP
8501 N. Scottsdale Road, Suite 270
Scottsdale, Arizona 85253
Telephone: (480) 428-0145
Facsimile: (866) 505-8036
gwotkyns@schneiderwallace.com

/s Gregory A. Cade
Gregory A. Cade
ENVIRONMENTAL LITIGATION GROUP, P.C.
2160 Highland Ave,
Birmingham, AL 35205
Telephone: (205) 328-9200
Facsimile: (205) 328-9456
GregC@elglaw.com

ATTORNEYS FOR THE COMMONWEALTH OF PUERTO RICO